

PATENT ABSTRACTS OF JAPAN

(11)Publication number : **09-204330**

(43)Date of publication of application : **05.08.1997**

(51)Int.Cl.

G06F 12/00

G06F 12/00

G06F 3/14

G06F 12/14

G09C 1/00

G09C 1/00

H04L 9/08

H04L 9/32

(21)Application number : **08-283854**

(71)Applicant : **HITACHI LTD**

(22)Date of filing : **25.10.1996**

(72)Inventor : **OTE ICHIRO**
IWABUCHI KAZUNORI
WASHIMI HIROAKI
FURUKAWA HIROSHI
SUMITOMO MASATO
KOBAYASHI YUICHI

(30)Priority

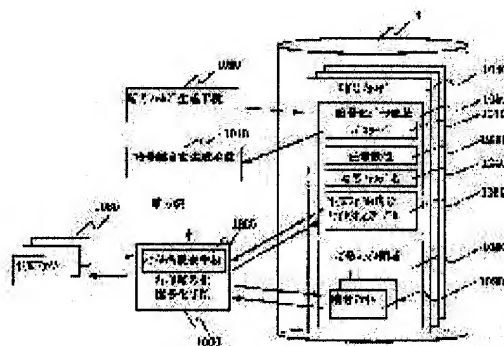
Priority number : **07279325** Priority date : **26.10.1995** Priority country : **JP**

(54) DEVICE AND METHOD FOR CIPHERING AND DECIPHERING INFORMATION

(57)Abstract:

PROBLEM TO BE SOLVED: To release a user from the managing of a cipher key and cipher file by generating a cipher folder on a storage device and allowing a ciphering and deciphering means to cipher a selected plain text file so as to automatically store and manage.

SOLUTION: When ciphering is instructed from the user, the file ciphering and deciphering means 1000 automatically generates the cipher key from the password 1070 of a cipher folder 1040 specified by the user by a cipher key automatic generation means 1010. Then through the use of the cipher key, the means 1000 ciphers a specified normal sentence file 1030 to store in a cipher file area 1080 in the cipher folder 1040 as a cipher file 1090. In addition, at the time of this storing, through the use of a file name converting means 1220, each file 1090 is stored by using individually unique internal name so as to make the cipher folder 1040 an area hidden from the user. At the time of deciphering, a corresponding normal sentence file 1030 and the name of the cipher file are stored in a plain text file/cipher file corresponding table 1060 so as to return to the original normal sentence file.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-204330

(43)公開日 平成9年(1997)8月5日

(51)Int.CI*	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 12/00	5 1 5		G 0 6 F 12/00	5 1 5 M
	5 3 7			5 3 7 H
3/14	3 7 0		3/14	3 7 0 A
12/14	3 2 0		12/14	3 2 0 B
G 0 9 C 1/00	6 3 0	7259-5J	G 0 9 C 1/00	6 3 0 A

審査請求 未請求 請求項の数18 O L (全 20 頁) 最終頁に続く

(21)出願番号 特願平8-283354

(22)出願日 平成8年(1996)10月25日

(31)優先権主張番号 特願平7-279325

(32)優先日 平7(1995)10月26日

(33)優先権主張国 日本 (J P)

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 大平 一郎

神奈川県川崎市麻生区王禅寺1090番地株式会社日立製作所システム開発研究所内

(72)発明者 岩瀬 一則

神奈川県川崎市麻生区王禅寺1090番地株式会社日立製作所システム開発研究所内

(72)発明者 鷺見 浩明

愛知県名古屋市中区榮三丁目10番22号日立中部ソフトウェア株式会社内

(74)代理人 弁理士 小川 勝男

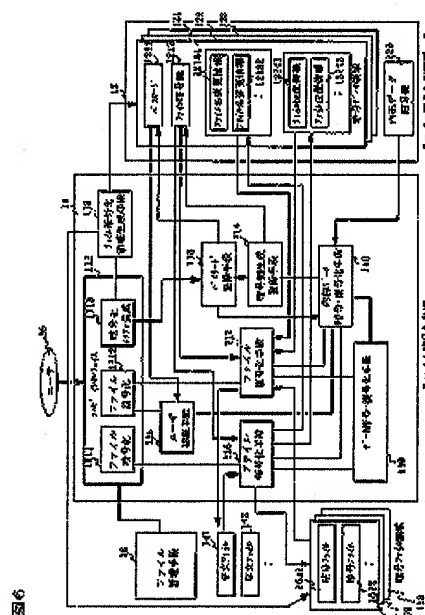
最終頁に続く

(54)【発明の名称】 情報の暗号化、復号化装置および方法

(57)【要約】 (修正有)

【課題】金庫を模倣しアイコンを対象として、ドラッグアンドドロップという直感的な操作により、ファイル暗号化の操作を実現し、さらに、ユーザ認証用のパスワードから自動的にファイルの暗号化・復号化に使う暗号鍵を生成し、暗号鍵に関する操作を一切ユーザから隠蔽するなど、エンドユーザ向けの簡単操作のファイル暗号化制御装置と方法を提供する。

【解決手段】暗号化・復号化を行うユーザ・インターフェイス部111と、パスワード1211から暗号鍵を自動生成する暗号鍵生成・登録手段114と、パスワードによる認証を行なうことなくファイル暗号処理をするファイル暗号化、復号化手段116、117とを備え、操作性の優れたファイル暗号化機能を提供する。



(2)

特開平9-204330

1

【特許請求の範囲】

【請求項1】 計算機上の情報の暗号化・復号化を行うデータ暗号化システムにおいて、ユーザが指定した平文ファイルを暗号鍵により暗号化、および、復号化するファイル暗号化復号化手段と、前記ファイル暗号化復号化手段により特定の暗号鍵を使用して暗号化した少なくとも一つの暗号ファイルを格納し、ファイルを管理するための暗号情報を格納する格納領域手段と、前記暗号情報格納領域手段にユーザがアクセスする際の認証パスワードを登録するためのパスワード登録手段を含む情報の暗号化、復号化装置。

【請求項2】 前記平文ファイルのファイル名を前記暗号情報格納領域手段の内部的な暗号ファイルのファイル名に変換するファイル名変換手段、前記平文ファイル名と前記暗号ファイル名とのファイル名対応テーブル、および、前記暗号情報格納領域手段に入力された暗号化に関連する内部データを暗号化するための内部データ暗号化復号化手段を含み、それにより前記暗号情報格納領域をユーザから隠蔽する請求項1記載の情報の暗号化、復号化装置。

【請求項3】 前記認証パスワードに基づき、前記暗号鍵を自動生成する暗号鍵自動生成手段を含み、前記ファイル暗号化復号化手段は、前記暗号鍵自動生成手段により自動生成した暗号鍵によりファイルの暗号化、および、復号化を行う請求項1記載の情報の暗号化、復号化装置。

【請求項4】 前記暗号情報格納領域手段に入力された、暗号化に関連する内部データを暗号化するための内部データ暗号化復号化手段を含み、前記認証パスワードを前記内部データ暗号化復号化手段により暗号化してパスワード登録手段の前記認証パスワード記憶領域に登録保持し、前記平文ファイルの暗号化の際に、前記認証パスワードを復号化し、前記暗号鍵自動生成手段により暗号鍵を自動生成し、前記暗号鍵を使用して、ファイルの暗号化を行う請求項3記載の情報の暗号化、復号化装置。

【請求項5】 特定回数以上入力された不正な認証パスワードがに回答して、前記暗号情報格納領域手段を無効化する暗号情報格納領域無効化手段を備える請求項1記載の情報の暗号化、復号化装置。

【請求項6】 前記暗号情報格納領域無効化手段により無効にした前記暗号情報格納領域手段を再び前記暗号情報格納領域手段として利用可能とするための暗号情報格納領域バックアップ手段を備える請求項5記載の情報の暗号化、復号化装置。

【請求項7】 記憶装置上に、前記暗号情報格納領域手段を複数生成し、前記暗号鍵、および、前記認証パスワードをそれぞれ独立に割り当てるための暗号情報格納領域生成手段を備える請求項1記載の情報の暗号化、復号化装置。

【請求項8】 前記暗号情報格納領域手段に格納された前

2

記暗号ファイルの暗号化以前の記憶装置上での位置情報テーブルを前記暗号情報格納領域手段に備え、前記暗号ファイルの復号化の際に、復号化後の平文ファイルを記憶装置上の元の位置に自動的に戻す請求項1記載の情報の暗号化、復号化装置。

【請求項9】 前記暗号情報格納領域手段の全てのデータを他の計算機に転送可能な外部ファイルに変換する外部ファイル変換手段、および、前記外部ファイルから前記暗号情報格納領域手段を再生成する暗号情報格納領域生成手段を備え、他の計算機への前記暗号情報格納領域手段の情報の転送を可能とする請求項1記載の情報の暗号化、復号化装置。

【請求項10】 他の計算機に転送して実行し、前記認証パスワードの入力により、前記暗号情報格納領域手段内の前記暗号ファイルを自動的に復号化可能な自己復号化プログラム・ファイルを前記暗号情報格納領域手段の全てのデータをファイル復号化処理プログラムに統合して生成する自己復号化プログラム生成手段を備える請求項1記載の情報の暗号化、復号化装置。

【請求項11】 ファイル暗号化の操作対象として計算機のディスプレイの画面上に金庫のような暗号装置を容易にイメージさせるグラフィック・メタファを表示し、ファイルの選択操作と前記グラフィック・メタファの選択操作という単純な連続操作に回答してファイルの暗号化を行うユーザ・インターフェイス手段を備える請求項1記載の情報の暗号化、復号化装置。

【請求項12】 計算機上の情報の暗号化及び復号化を装置を用いて行う情報の暗号化、復号化方法は以下のステップを含む：前記情報としての平文ファイルを暗号化した暗号化ファイルを記憶する暗号化ファイル領域と、平文ファイル名と暗号化ファイル名とを対応させて記憶する暗号化データ領域と、ユーザが入力したパスワードをシステム鍵によって暗号化したパスワードを記憶するパスワード記憶領域とを特定した記憶エリア（記憶フォルダ）を設けること；暗号化において、

暗号化ユーザが入力したパスワードをシステム鍵を用いて暗号化パスワードを生成し、前記パスワード記憶領域に記憶すること；暗号化パスワードをシステム鍵によって復号化し、暗号鍵を生成すること；前記暗号鍵を用いて、指定された平文ファイルを暗号化して、暗号化平文ファイルを前記暗号化ファイル領域に格納すること；および平文ファイル名と暗号化ファイル名の対応を表わすテーブルを前記暗号化データ領域に登録すること；復号化において、

復号化ユーザが入力したパスワードに基づき、暗号化データ領域の前記登録対応テーブルを表示すること；前記表示テーブルを参照して、復号化すべきファイル名をユーザにより指定すること；前記入力パスワードに基づき、前記復号鍵を生成すること；前記生成した復号鍵を用いて、前記指定されたファイル名の暗号化ファイルを

(3)

特開平9-204330

3

4

復号化すること。

【請求項13】請求項12情報の暗号化、復合化方法において、前記復号化において、復号化ユーザーのパスワードの入力に応じて、その入力したパスワードを、前記パスワード記憶領域に記憶されたパスワード照合し、認証の結果に応じて、復号化プロセスの実行を許否する。

【請求項14】請求項12情報の暗号化、復合化方法において、前記記憶エリアを複数設定し、各エリアを区別化して表わすメタファイルにより、表示画面上に表示

【請求項15】請求項14情報の暗号化、復合化方法において、前記表示画面上に表示されたファイル名をポインティング装置により指定し、かつ重畳関係で該装置で前記複数記憶エリアを表示するアイコンの1つを特定することにより、復号化操作（プロセス）を起動することを含む。

【請求項16】請求項12情報の暗号化、復合化方法において、前記復号化において、前記ファイル名は記憶エリア内の暗号ファイル領域に格納された暗号化されたフ

【請求項17】計算機上で、情報の暗号化及び復号化の動作を指示するための計算機で読み取り可能なメモリ媒体は以下を含む：前記情報としての平文ファイルを暗号化した暗号化ファイルを記憶する暗号化ファイル領域と、平文ファイル名と暗号化ファイル名とを対応させて記憶する暗号化データ領域と、平文ファイル名と暗号化ファイル名とを対応させて記憶する暗号化データ領域と、ユーザが入力したパスワードをシステム鍵によって暗号化したパスワードを記憶するパスワード記憶領域とを特定した記憶エリア（記憶フォルダ）を設ける手段；

暗号化ユーザが入力したパスワードをシステム鍵を用いて暗号化パスワードを生成し、前記パスワード記憶領域に記憶する手段；暗号化パスワードをシステム鍵によって復号化し、暗号鍵を生成する手段；前記暗号鍵を用いて、指定された平文ファイルを暗号化して、暗号化平文ファイルを前記暗号化ファイル領域に格納する手段；および平文ファイル名と暗号化ファイル名の対応を表わすテーブルを前記暗号化データ領域に登録する手段；復号

化において、復号化ユーザが入力したパスワードに基づき、暗号化データ領域の前記登録対応テーブルを表示する手段；前記表示テーブルを参照して、復号化すべきファイル名をユーザにより指定する手段；前記入力パスワードに基づき、前記復号鍵を生成する手段；前記生成した復号鍵を用いて、前記指定されたファイル名の暗号化ファイルを復号化する手段。

【請求項18】請求項17の媒体において、前記復号化において、復号化ユーザのパスワードの入力に応じて、

その入力したパスワードを、前記パスワード記憶領域に記憶されたパスワードと照合し、認証の結果に応じて、復号化プロセスの実行を許否する手段を含む。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、個人情報や秘密情報を暗号化して保持し、第三者への情報漏洩を防止する情報システムと方法に関する。

【0002】

【従来の技術】ノート型パーソナルコンピュータ（以後、PCと称す）やペン入力PC等、高性能、かつ、携帯性の高い計算機の普及により、出張先等、事務所外でのさまざまな場所で、計算機を業務を目的として利用する機会が増加してきている。こうした携帯型の計算機の普及に伴って、計算機の盗難、紛失による情報漏洩が問題となりつつある。

【0003】一方、マルチメディア化等に伴って家庭でもPCを始めとする計算機が普及してきている。このような家庭向けの計算機では、家族で共有して計算機を使うことが多く、個人情報の保護機能が必要となりつつある。

【0004】こうした計算機の携帯化や家庭への浸透等により、業務に関連した機密情報や個人情報の漏洩に対するエンドユーザ・レベルでのセキュリティ機能に対するニーズが高まりつつある。

【0005】これらのニーズに対応したセキュリティ機能としては、機密情報ファイルや個人情報ファイルを暗号鍵を用いて暗号化して、暗号鍵を所持しない第三者からの情報アクセスから保護するファイルの暗号化機能が、有効な手法として知られている。

【0006】

【発明が解決しようとする課題】ところで、従来のファイル暗号化機能では、第三者に秘密とする暗号鍵を暗号処理に用いるため、ファイル暗号化や復号化の際に、パスワードの入力による暗号鍵のオープン操作等の準備操作が必要であったり、暗号鍵の管理をユーザが行う必要があった。また、暗号化したファイルの管理についてもユーザに任されており、例えば、ファイルを後で復号化するためにどの暗号鍵で暗号化したファイルかをユーザ責任で記憶しておく必要があった。このように従来のファイル暗号化機能は、専門知識を必要としたり、操作が複雑でエンドユーザには操作が難しく、気軽に利用できないという問題があった。したがって、ファイル暗号化等の高度なセキュリティ機能は、一般に、一部の専門的な業務を行うユーザ向けのものとなっていた。

【0007】本発明者は、暗号鍵を自動生成することによりユーザが暗号鍵を意識することなくファイルの暗号化復号化を行えること、また、特定の暗号鍵により暗号化した暗号ファイルを一括管理することによりユーザの一つ一つの暗号ファイルの管理が不要になること、さら

(4)

特開平9-204330

5

に、ファイルの復号化の操作の際にのみユーザの認証を行えば必ずしも暗号化の操作の際にユーザの認証を行わなくても暗号化したファイルの保護を行えることに着目した。

【0008】従って、本発明は、上記着目点に基づき、暗号鍵と暗号ファイルの管理からユーザを解放し、また、画面上で平文ファイルを選択しアイコン等のグラフィック・メタファにより暗号化処理を起動するという単純な操作で、ファイルの暗号化を可能とする情報の暗・復号化装置と方法を提供することを目的とする。

【0009】

【課題を解決するための手段】上記目的を達成するために、本発明の一つの態様による情報の暗・復号化装置は、ユーザが指定した平文ファイルを暗号鍵により暗号化、および、復号化する暗号化復号化手段と、特定の暗号鍵を使用して前記暗号化復号化手段により暗号化した暗号ファイルを一括して格納・管理する記憶装置上の暗号情報格納手段（以後、暗号フォルダと呼ぶ）と、記憶装置上に前記暗号フォルダを複数生成し、前記暗号鍵、および、前記認証パスワードをそれぞれ独立に割り当てる暗号フォルダ生成手段と、前記暗号フォルダにユーザがアクセスする際の認証を行うための認証パスワードを格納する格納手段を含む。

【0010】さらに、本発明の別の態様によれば、前記暗号化制御装置は、前記暗号フォルダ内部の暗号化に関連する内部データを暗号化するための内部データ暗号化復号化手段と、前記平文ファイルのファイル名を前記暗号フォルダの内部的な暗号ファイル名に変換するファイル名変換手段と、前記暗号フォルダ内部に前記平文ファイル名と変換した前記暗号ファイル名との対応テーブルを含む。

【0011】本発明の別の態様によれば、前記暗号化制御装置は、前記認証パスワードを基に暗号鍵を自動生成する暗号鍵自動生成手段と、前記暗号フォルダ内部に、認証パスワードを登録保持するための認証パスワード記憶領域を含む。

【0012】本発明による暗号化制御装置の動作の概要を説明すると、あらかじめ、前記暗号フォルダ生成手段により記憶装置上に暗号フォルダを生成しておくことで、ユーザが選択した平文ファイルは、前記暗号化復号化手段が前記暗号フォルダに割り当てられた前記暗号鍵を使用して暗号化し、自動的に前記暗号フォルダ内に格納して、一括して記憶・管理するために、ユーザによる暗号ファイル毎の個別的な管理を不要とすることができ、また、前記暗号化復号化手段は、ユーザが暗号フォルダにアクセスしてファイルの暗号化・復号化を行う際に、それぞれ前記暗号フォルダに割り当てられた前記認証パスワードにより、正しいユーザが否か認証を行い、前記暗号フォルダに対する不正アクセスから保護する。

【0013】前記暗号フォルダ内に格納された前記暗号

6

ファイル名は、前記ファイル名変換手段により、ユーザが認識している前記平文ファイルから内部的な暗号ファイルに変換し、また、前記暗号フォルダ内部の暗号ファイルを記憶・管理するための内部データについても、前記内部データ暗号化復号化手段により暗号化すること、前記暗号フォルダに格納された前記暗号ファイルをユーザから隠蔽し、内部データに対するユーザの不正なアクセスや誤操作から保護可能となる。

【0014】前記暗号鍵自動生成手段は、前記暗号フォルダにアクセスするためにユーザが入力した前記認証パスワードを基に前記暗号鍵を自動生成し、煩雑なユーザによる前記暗号鍵の操作・管理を不要とする。

【0015】さらに、暗号化フォルダ生成時に、前記暗号フォルダ生成手段が前記暗号フォルダ内部に前記認証パスワード記憶領域を設定し、ユーザが入力した前記認証パスワードを前記内部データ暗号化復号化手段により暗号化して前記認証パスワード記憶領域に登録・保持した場合には、前記暗号化復号化手段は、前記認証パスワード入力による認証を省略して、前記前記認証パスワード記憶領域に登録した前記認証パスワードを読み出し、前記内部データ暗号化復号化手段により復号化して、前記暗号鍵自動生成手段により暗号鍵を自動生成してファイルの暗号化を行う。したがって、ユーザは、前記認証パスワードの入力を行うこともなく平文ファイルを選択して前記暗号化復号化手段を起動するといった非常に単純な操作でファイルの暗号化を行うことが可能となる。

【0016】特に、前記暗号フォルダ生成手段が、前記暗号フォルダ生成時に、金庫等の暗号装置をユーザにイメージさせるアイコン等のグラフィック・メタファを前記暗号フォルダ毎に計算機の画面上に表示し、さらに、前記グラフィック・メタファの選択操作を契機に前記暗号化復号化手段が起動するようにしておくと、マウス等のポインティングデバイスにより画面上でファイル管理機能から平文ファイルを選択し、そのまま、前記グラフィック・メタファを選択するという画面上での単純で直感的な操作によりファイルの暗号化が可能となり、一般ユーザ向けの操作性の良い暗号化機能を提供できる。

【0017】

【発明の実施の形態】以下、本発明の実施例を図面を参照して説明する。図2は、本発明の暗号化制御装置を実現するシステムの基本構成を示す。1はCPU、2はROM、3はRAM、4はディスク装置、5はディスプレイ装置、6はキーボード、7はマウス、8はシステム・バスを表わす。本発明を実現する各制御プログラムはあらかじめディスク4上に格納し、RAM4上にロードし、CPU1により制御実行する。また、各データ領域は、RAM4上で処理した後に、保存の必要なデータは、ディスク4上に格納する。

【0018】図1は、本発明を実現する一実施例のブロック図を示し、本発明の基本構成について説明する。1

(5)

特開平9-204330

7

000は、暗号鍵を用いて、ファイルの暗号化と復号化を行うファイル暗号化復号化手段、1220は、平文ファイル名から内部的な暗号ファイル名にファイル名を変換するファイル名変換手段、1010は、本発明の特徴となるパスワードからの暗号鍵の自動生成を行う暗号鍵自動生成手段を表わし、1030は、暗号化の対象となる平文ファイル、1040は、ディスク4上の本発明の特徴となる暗号フォルダを表わし、暗号フォルダは平文1030を暗号化した暗号ファイル1090を格納する暗号ファイル領域1080と前記暗号フォルダ1040を管理するための情報を格納する暗号化データ領域1050から構成する。また、暗号化データ領域1050は、暗号化する前の平文ファイル名と暗号化後の暗号ファイル名の対応を管理するための平文ファイル/暗号ファイル対応テーブル1060、ユーザが暗号フォルダにアクセスするための認証に使うパスワード1070、暗号鍵自動生成手段1010が、パスワード1070から暗号鍵を自動生成する際に使用する任意数値1230、暗号フォルダ名1240を格納し、それぞれの格納領域を含む。1020は、暗号フォルダ1040を生成する暗号フォルダ生成手段を表わし、ディスク4上に複数の暗号フォルダの生成を可能とする。

【0019】本実施例では、ファイルの暗号化を行うために、初期設定として暗号フォルダ生成手段1020により、ディスク4上に、一つ以上の暗号フォルダ1040を生成する。暗号化フォルダ生成手段1020は、ディスク4上に、暗号フォルダ1040を構成するディレクトリを生成し、そのディレクトリ内に、暗号化データ領域1050を構成するファイルと暗号ファイル領域1080を構成するサブディレクトリを作成する。さらに、暗号フォルダ1040作成時には、ユーザに対して、パスワード1070、任意数値1230、暗号フォルダ名1240の入力を要求し、ユーザが入力したパスワード1070、任意数値1230、暗号フォルダ名1240を暗号化して、暗号化データ領域1050に格納する。暗号化データ領域1050に格納するデータの暗号化は、参照できないようにするため、これら内部データの暗号化専用用意した暗号鍵により行う。

【0020】ファイル暗号化復号化手段1000が暗号化を行うための暗号鍵は、暗号化あるいは復号化を行う際に、暗号鍵自動生成手段1010が、暗号化データ領域1050に暗号化して格納したパスワード1070と任意数値1230から生成する。暗号鍵自動生成手段1010は、パスワード1070と任意数値1230を取り出し、復号化して、これらに適当なビットシフト等のビット操作や演算を施しながら合成し、暗号フォルダ毎にユニークな暗号鍵を自動的に生成する。任意数値1230は、パスワード1070から暗号鍵を生成するために十分なビットサイズを持った数値とし、暗号フォルダ1040生成時に一度だけユーザから入力する。また、

8

暗号鍵は、後述する実施例のように、暗号フォルダ生成時に、暗号鍵自動生成手段1010が、登録されたパスワード1070から自動生成し、パスワードと共に暗号化データ領域1050に暗号化して格納する方法もある。この場合、暗号化の際に、登録した暗号鍵を利用できるので、逐次、暗号鍵を生成する必要はない。

【0021】平文ファイル1030の暗号化は、ファイル暗号化復号化手段1000によって行う。ユーザからのファイル暗号化の指示があるとファイル暗号化復号化手段1000は、まず、暗号鍵自動生成手段1010によりユーザが指定した暗号フォルダ1040のパスワード1070から暗号鍵を自動生成する。そして暗黙に自動生成した暗号鍵を使用して、ユーザが指定した平文ファイル1030を暗号化して暗号フォルダ1040の暗号ファイル領域1080に暗号ファイル1090として格納する。このように、暗号フォルダ生成時に、あらかじめ、暗号フォルダ1040内にパスワード1070を格納しておき、それを基に暗号鍵を自動生成し、その暗号鍵によりファイルの暗号化を行うことにより、ユーザがパスワード入力による認証や暗号鍵のオープン処理等することなく、ファイル選択とファイル暗号化復号化手段1000の起動という単純な操作だけでファイルの暗号化が可能となる。

【0022】また、ファイル暗号化復号化手段1000は、暗号ファイル1090を格納する際、ファイル名変換手段1220により暗号ファイル1090ごとにそれぞれユニークな内部名を生成し、その名前を使って、暗号ファイル1090を暗号ファイル領域1080に格納して、暗号フォルダ1040をユーザから隠蔽された領域とする。復号化の際に、元の平文ファイルに戻すために、対応する平文ファイル1030の名前と暗号ファイル1090の名前を暗号化データ領域1050の平文ファイル/暗号ファイル対応テーブル1060に格納する。このように、内部データ暗号化用の暗号鍵による暗号化データ領域1050の暗号化、および、ファイル名変換手段1220と平文ファイル/暗号ファイル対応テーブル1060による暗号ファイル名の変換で、暗号フォルダ1040をユーザから隠蔽し、暗号ファイルや暗号鍵の管理からユーザを解放する。

【0023】平文ファイル1030の復号化も、ファイル暗号化復号化手段1000によって行う。

【0024】復号化するために、ファイル暗号化復号化手段1000を起動すると、ファイル暗号化復号化手段1000は、ユーザ入力パスワードに対するパスワード1070による認証処理を行った後、平文ファイル/暗号ファイル対応テーブル1060を参照して、暗号ファイル領域1080内の暗号ファイル1090を平文ファイル名で一覧表示する。この状態は、暗号フォルダ1040をオープンした状態で、ユーザは、平文ファイル名での一覧表示の中から暗号ファイル領域1080内の暗

(6)

特開平9-204330

9

号ファイル1090を選択し、復号化できる。ユーザが、一覧から暗号ファイル1090を一つ以上選択して、再び、ファイル暗号化復号化手段1000を起動すると、ファイル暗号化復号化手段1000は、まず、暗号鍵自動生成手段1010によりパスワード1070から暗号鍵を自動生成する。次に平文ファイル/暗号ファイル対応テーブル1060を参照して、ファイル名変換手段1220によりユーザが選択した平文ファイル名を暗号ファイル1090の名前に変換して、暗号ファイル領域1080から取り出す。さらに、自動生成しておいた暗号鍵を使用して復号化し、元の平文ファイル名の平文ファイルに戻す。

【0025】このように、ファイルの復号化の際にも暗号鍵自動生成手段1010やファイル名変換手段1220と平文ファイル/暗号ファイル対応テーブル1060により、暗号鍵を意識することなく、パスワード1070の入力、平文ファイル名による暗号ファイルの選択、そして、ファイル暗号化復号化手段1000の起動という単純な操作だけでファイルの復号化が可能なる。

【0026】次に、FD (Floppy Disk) 等の媒体やネットワークを通して暗号フォルダを他の計算機への転送することを目的として、暗号フォルダの外部ファイルへの交換を行う実施例について図3により説明する。図3の暗号化フォルダ1040は、図1の暗号化フォルダと同一のものである。ユーザから暗号フォルダの外部ファイルへの交換を要求されると、暗号フォルダ・ファイル生成手段1100は、ユーザが選択した暗号フォルダ1040に対応する暗号化データ領域1050、暗号ファイル領域1080のディレクトリの暗号ファイル1090のデータをそれぞれ読み出し、1ファイルに結合して、暗号フォルダ・ファイル1120を作成する。暗号フォルダ・ファイル1120は、外部ファイルとしてディスク4上の特定のディレクトリやFD1300に出力する。

【0027】暗号フォルダ・ファイル1120は、FD1300やネットワーク1400等を介して、本発明の概念に従うファイル暗号化機能をあらかじめ設定した計算機に転送し、暗号フォルダ生成手段1110により再び暗号フォルダ1040に復帰できる。暗号フォルダ生成手段1110は、暗号フォルダ・ファイル1120から暗号化データ領域1050と暗号ファイル領域データ1130のデータをそれぞれ読み出して、このデータを基に、暗号フォルダ生成手段1020と同様に、転送先の計算機に接続されたディスク4上に暗号化フォルダ1040を生成する。この暗号フォルダに格納された暗号ファイルは、図1の実施例とまったく同様に、パスワードを入力することで復号化することが可能となる。

【0028】図3の実施例では、暗号フォルダ・ファイル1120として1ファイルとしたが、計算機のオペレーティングシステム(OS)がディレクトリ毎の転送を支援するような場合は、暗号フォルダのディレクトリ内の

10

ファイルやディレクトリを適当なディレクトリにまとめて外部ファイル群としてFD1300等の媒体に格納することもちろん可能である。

【0029】また、図3の実施例のように、暗号フォルダ・ファイル1120を1ファイルで構成した場合、内部に複数暗号ファイルのデータを含むことから暗号フォルダ・ファイル1120のサイズが大きくなる場合がある。この場合、暗号フォルダ・ファイル生成手段1100により暗号フォルダ・ファイル1120を生成する際に、データ圧縮処理を行い、再び、暗号フォルダ生成手段1110により暗号フォルダ1040を生成する際に、伸長処理を行う等により、暗号フォルダ・ファイル1120のサイズの縮小化を図ることが可能である。

【0030】ところで、図3の実施例では、暗号フォルダ・ファイル1120を転送する計算機に、本発明の概念に従うファイル暗号化システムをあらかじめ設定されていることが前提となっていた。これは任意の計算機に暗号ファイルを配布するような場合に不便である。そこで、図4の他の実施例では、本発明概念のファイル暗号化システムがあらかじめ設定されていない計算機上でも暗号フォルダ・ファイル内の暗号ファイルを展開できるようにする。

【0031】自己復号化ファイル生成手段1140は、暗号フォルダ1040の暗号化データ領域1050、暗号ファイル1090のデータをそれぞれ読み出し、結合する。さらに、これを復号化対象のデータとして、ファイル暗号化復号化手段1000の復号化処理と等価な機能を持つ復号化手段1170と暗号鍵自動生成手段1010とで構成する復号化プログラム1150のファイルに連結して、自己復号化プログラム1160のファイルを生成する。自己復号化プログラム1160は、外部ファイルとしてディスク4上の特定のディレクトリやFD1300に出力する。

【0032】自己復号化プログラム1160を他の計算機に転送して実行すると、復号化手段1170が起動される。復号化手段1170は、内部データとして結合された暗号フォルダ1040のデータから暗号化データ領域1050と暗号ファイル領域データ1130のデータをそれぞれ読み出す。そしてユーザにパスワード入力を要求し、パスワード1070と照合し、正しいパスワードなら、復号化の処理を開始する。パスワード1070から暗号鍵を自動生成して、暗号ファイル1090のデータを復号化していく処理は、図1の実施例と同様である。転送先の計算機に接続されたディスク4上の、例えばユーザが指定したディレクトリに、復号化した平文ファイル1030を出力して、必要なら、最後に、自己復号化プログラム1160自体をディスクから削除し、自己復号化処理を終了する。本実施例により、プログラム実行の可能な任意の計算機のユーザにネットワーク1400を介して暗号ファイルを暗号フォルダ単位で転送可

11

能となり、本発明の応用範囲が非常に広がる。

【0033】次に、暗号フォルダへの不正なアクセスを防止をするための不正パスワード入力回数の限定方法について図5を用いて説明する。図5のファイル暗号化復号化手段1000、鍵自動生成手段1010、暗号フォルダ生成手段1020、暗号フォルダ1040は、図1と同一構成である。1180は、暗号フォルダ1040へユーザがアクセスする際に、パスワードで、ユーザ認証を行うための認証手段。1190は、認証手段1180が、不正なパスワードの入力回数をカウントするためのカウンタ、1200は、ユーザから不正なパスワードが入力された場合に、暗号化フォルダ1040を無効にして暗号フォルダ1040への不正なアクセスを防止をするための暗号フォルダ無効化手段。1210は、暗号フォルダ無効化手段1200により無効にした暗号フォルダ1040を復帰するために、無効化される前に、暗号化フォルダをバックアップしておくための暗号フォルダ・バックアップ手段を表わす。

【0034】ファイル暗号化復号化手段1000は、暗号フォルダ1040内の暗号ファイル1090の復号化等を行う際、認証手段1180により、暗号フォルダ1040にアクセスするためのパスワード入力をユーザに要求する。ユーザからパスワードが入力されると、認証手段1180は、暗号フォルダ内のパスワード1070と比較して、一致した場合、正当なユーザと判断し、ファイル暗号化復号化手段1000の処理を進める。一方、不正なパスワードが入力されると、認証手段1180は、カウンタ1190をカウントアップしていく。但し、カウンタ1190は、正しいパスワードが入力された時点で、クリアする。不正なパスワードが連続して入力され、カウンタ1190の値があらかじめ設定された特定回数、例えば、3回を越えると認証手段1180は、暗号フォルダ無効化手段1200に、暗号フォルダ1040を無効にするように指示する。

【0035】暗号フォルダ無効化手段1200は、認証手段1180から指示を受けると、暗号フォルダ1040内のパスワード1070を消去する。認証手段1180は、パスワード1070が消去されていること確認すると認証処理を中止して、ユーザに、暗号フォルダが無効であることをメッセージとして知らせる。したがって、一旦、パスワード1070が消去されると、以後、暗号フォルダ1040へのアクセスは不可能となる。

【0036】無効化されると正当なユーザでも暗号フォルダ1040へアクセスできなくなるため、正当なユーザが無効となった暗号フォルダ1040を復帰させる手段が必要となる。そこで、暗号フォルダバックアップ手段1210は、暗号化フォルダ1040をバックアップする機能を提供する。

【0037】暗号フォルダバックアップ手段1210

(7)

特開平9-204330

12

は、暗号フォルダ1040のバックアップの際に、パスワード1070の内容を、例えば、FD1300のようなリムーバブルな媒体にコピーする。さらに、暗号フォルダ名1240を暗号フォルダ1040を特定する情報としてFD1300に記録する。復帰の際には、暗号フォルダ名1240と比較して、バックアップされているFD1300の内容と暗号フォルダ1040が一致していることを確認し、FD1300にバックアップされたパスワード1070を暗号フォルダ1040にコピーし、暗号フォルダ1040を元の状態に戻す。

【0038】バックアップに使用したFD1300が不正な復帰処理に使われることを防止するには、FD1300による復帰の際に、暗号フォルダ名1240と比較した後、ユーザにパスワード入力を要求し、FD1300内のパスワード1070との一致をチェックすることにより、第三者による不正な復帰処理を防止できる。

【0039】この暗号フォルダバックアップ手段1210により、ユーザは、暗号化フォルダ1040が無効化に備え、事前に暗号フォルダのバックアップをFD1300等にとって置くことで、暗号フォルダ1040が不正なパスワード入力により無効化された場合でも、FD1300を使って暗号フォルダ1040を復帰し、再び、アクセスすることが可能となる。

【0040】また、暗号フォルダバックアップ手段1210のバックアップ操作は、パスワードによる認証後に可能とし、復帰操作は、随時行えるようにすることで、正当なユーザのみが暗号フォルダ1040をバックアップし、無効化された状態でも復帰可能となり、第三者による不正なバックアップを防止することができる。

【0041】図6に、本発明の一実施例のブロック図を示し、さらに詳細に説明する。

【0042】11は、本発明を實現するファイル暗号化制御プログラムである。111は、ユーザがファイル暗号化を行うためのユーザ・インターフェイス部である。

1111は、ファイル暗号化のユーザ・インターフェイスである。このユーザ・インターフェイス1111は、本発明特徴となる簡便なファイル暗号化の操作を實現する。1112は、ファイル復号化のユーザ・インターフェイスである。1113は、ユーザがファイル暗号化を行うための操作対象となるメタファを登録するファイル暗号化メタファ登録のユーザ・インターフェイスである。この暗号化のメタファを用いて、ユーザ・インターフェイス1111は、前述の簡便なファイル暗号化の操作を實現する。112は、ファイル暗号化に必要なデータ領域をディスク4上に確保するファイル暗号化領域生成手段である。113は、ユーザの認証に必要なパスワードをあらかじめ登録するパスワード登録手段である。114は、ファイルの暗号化に必要な暗号鍵を生成し、登録する暗号鍵生成・登録手段である。この暗号鍵生成・登録手段は、ユーザが入力したパスワードを用い

(8)

特開平9-204330

13

て、本実施例の特徴である暗号鍵の自動生成を行う。115は、ユーザが入力したパスワードとあらかじめ登録したパスワードを比較してユーザの認証を行うユーザ認証手段である。116は、ファイル単位で暗号化を行うファイルの暗号化手段である。117は、ファイル単位で復号化を行うファイル復号化手段である。118は、暗号化したファイルの機密性を保持するために内部データの暗号化を実現する内部データ暗号・復号化手段である。119は、与えられた暗号鍵を用いてデータを暗号・復号化するデータ暗号・復号化手段である。

【0043】12は、ファイル暗号化制御プログラム11を制御するためのファイル暗号化制御データである。このファイル暗号化制御データは、メモリ上で処理し、システム再スタート時にも有効とするためディスク4上に保存する。121、122、123は、ファイル暗号化制御データ12の内、暗号化したファイルの機密性を保持するために、暗号化してディスク4に格納する必要のある制御データを格納する暗号データ領域である。1211は、ユーザが入力したパスワードのデータ。1212は、自動生成したファイル暗号鍵のデータ。12131、12132は、暗号化したファイルをユーザから隠蔽するために名前を変更した際の元の平文ファイル名と変更後の暗号ファイル名の対応関係を保持したファイル名変更情報。12141、12142は、暗号化した平文ファイルが暗号化する前に存在したディスク4上でのファイル位置情報である。120は、内部データを暗号化するための内部データ暗号鍵である。

【0044】13は、ユーザがディスク装置4上のファイルを実行・管理するための管理機能を提供するファイル管理手段である。

【0045】141、142は、ディスク4上に格納され、暗号化の対象となる平文ファイルである。本実施例では、暗号化する平文ファイル141、142等をユーザの指示に従って、ファイル暗号化制御プログラム11に対して、通知するためにファイル管理手段を利用する。

【0046】151、152、153は、暗号化したファイルのデータ1511、1512等を格納するために、ディスク4上に確保した暗号ファイル領域である。

【0047】図6の構成要素と図1の構成要素の対応関係は、ファイル暗号化領域生成手段112、パスワード登録手段113は、暗号フォルダ生成手段1020に、暗号鍵生成・登録手段114は、暗号鍵自動生成手段1010に、ファイル暗号化手段116、ファイル復号化手段117、データ暗号・復号化手段119は、ファイル暗号化・復号化手段1000に、暗号データ領域121、122、123は、暗号化データ領域1050に、パスワード1211は、パスワード1070に、ファイル名変更情報12131、12132は、平文ファイル／暗号ファイル対応テーブル1060に、平文ファイル1

14

41、142は、平文ファイル1030に、暗号ファイル領域151、152、153は、暗号ファイル領域1080に、暗号1511、1512は、暗号ファイル1090に、それぞれ対応する。

【0048】次にファイル暗号化メタファ登録の手順、ファイル暗号化の手順、ファイル復号化の手順についてフローチャートを用いて説明する。

【0049】図7は、ファイル暗号化メタファ登録時の処理手順をフローチャートで示す。ユーザがユーザ・インターフェイスである暗号化メタファ生成手段（プログラム）1113を操作してファイル暗号化メタファ登録処理を起動すると（ステップ5001）、ユーザ・インターフェイス1113は、まず、ファイル暗号化領域生成手段112を制御して、暗号データ領域121をディスク4上のファイルとして、暗号ファイル領域151をディスク4上のディレクトリとして作成する（ステップ5002）。これらのファイル、および、ディレクトリは、例えば、暗号化制御プログラム11を格納したディスク4上のディレクトリ下に作成する。また、本実施例では、ユーザがユーザ・インターフェイス1113により暗号化のためのメタファを複数生成することを可能とするため、ユーザが、メタファの生成を行う毎に、ファイル暗号化領域生成手段112によって、暗号化データ領域122、123等を、また、暗号ファイル領域152、153等を随時生成していく。これにより、ユーザは、それぞれ独立したメタファを操作して、独立に設定したおいた暗号化ファイルの格納領域にファイル分類して格納することが可能となる。ユーザは、例えば、ユーザ毎またはファイル種類毎に、ファイルを分類して暗号化し、保存することが可能となる。次に、ユーザ・インターフェイス1113は、ユーザにパスワード入力要求する（ステップ5003）。ユーザが入力したパスワードは、パスワード登録手段113に渡す。パスワード登録手段113は、ユーザが入力したパスワードを内部データ暗号鍵120を用いて、内部データ暗号・復号化手段118により暗号化する。内部データ暗号・復号化手段118は、データ暗号・復号化手段119によりデータの暗号化を行う。パスワードを暗号化するとパスワード登録手段113は、パスワード1211としてディスク4に格納する（ステップ5004）。パスワード登録手段113は、パスワードの登録が終わると、暗号化する前のパスワードを暗号鍵生成・登録手段114に渡す。パスワードが渡されると暗号鍵生成・登録手段114は、例えば、パスワードとあらかじめ各暗号データ領域に対してユニークになるように割り当てられた数値とを合成し、ビット操作等を行うことにより、暗号鍵を自動的に生成する。さらに、暗号鍵生成・登録手段114は、生成した暗号鍵を内部データ暗号鍵120、および、内部データ暗号・復号化手段118により暗号化して、ファイル暗号鍵1212としてディスク4に格納す

(9)

特開平9-204330

15

る(ステップ5005)。以上のような暗号ファイル領域151、152、153、および、暗号データ領域121、122、123の生成・登録処理を終了すると、最後に、ファイル暗号化を行うためのメタファの登録処理を行う(ステップ5006)。このメタファの登録に関しては、後述の実施例で説明する。

【0050】次に、図8のフローチャートにより、ファイル暗号化時の処理手順について説明する。前述の暗号化メタファの登録処理を行った後、ユーザが、ファイル暗号化制御プログラム11を実行すると(ステップ6001)、ユーザ・インターフェイス111は、まず、ユーザがファイル暗号化処理の操作を行うためのファイル暗号化のメタファを表示する。ユーザが、マウス7のようなポインティング・デバイスを操作して、ファイル管理手段13のユーザ・インターフェイス上で暗号化する平文ファイルを選択し、さらに、続けて、ファイル暗号化メタファを選択すると、ユーザ・インターフェイス111は、選択された平文ファイルを対象として、ファイル暗号化処理を開始する(ステップ6002)。これらのユーザ・インターフェイスについては、後述の実施例で詳しく説明する。ところで、例えば、平文ファイル141が選択された場合、まず、ユーザ・インターフェイス111は、平文ファイル名をファイル暗号化手段116に渡す。ファイル暗号化手段116は、暗号化する平文ファイル名141を受け取ると、暗号ファイル名を作成する(ステップ6003)。この暗号ファイル名は、暗号化したファイルに対してそれぞれユニークになるように、例えば、暗号化処理の回数のカウント値等から作成したシリアル番号と特定文字を組み合わせて生成する。次に、復号化の際に、元の平文ファイル名に戻すため、暗号ファイル名と141の平文ファイル名のセットを内部データ暗号鍵120と内部データ暗号・復号化手段118により暗号化した後、ファイル名変更情報12131としてディスク4に格納する(ステップ6004)。次に、ファイル暗号化手段116は、平文ファイル141のディスク4上での位置情報(平文ファイル141が格納されていたディレクトリの位置情報)を内部データ暗号鍵120と内部データ暗号・復号化手段118により暗号化した後、ファイル位置情報12141としてディスク4に格納する(ステップ6005)。次に、平文ファイル141のデータをディスク4より読みだし、内部データ暗号鍵120と内部データ暗号・復号化手段118により復号化したファイル暗号鍵1212を用いて、データ暗号・復号化手段119により暗号化し、暗号ファイル・データ1511として、ディスク4に格納する(ステップ6006)。以上がファイルの暗号化処理である。複数の平文ファイルを対象として、ファイル暗号化処理を開始した場合には、ステップ6003～ステップ6005の処理を繰り返す(ステップ6007)。ただし、以上の手順は一例であり、特に複数フ

16

ァイルを暗号化する場合、手順を変えて、複数ファイルに対するファイル名変更情報やファイル位置情報等をまとめて暗号化して格納する等により、さらに、処理を高速化する等の工夫も本発明において可能なことは、言うまでもない。

【0051】次に、図9のフローチャートにより、ファイル復号化時の処理手順について説明する。例えば、ファイル暗号化のメタファを指して、マウス押下を2回連続的に行う(以後、ダブルクリックと称す)等の操作を行い、ユーザ・インターフェイス1112に対して起動をかけると、ユーザ・インターフェイス1112は、ファイル復号化処理を開始する(ステップ7001)。これらのユーザ・インターフェイスについては、後述の実施例で詳しく説明する。ユーザ・インターフェイス1112は、ファイル復号化の処理として、まず、ユーザの認証を行うために、ユーザにパスワードの入力を要求する(ステップ7002)。ユーザがパスワード入力すると、ユーザ・インターフェイス1112は、そのパスワードをユーザ認証手段115に渡す。ユーザ認証手段115は、パスワードを受け取ると、暗号化されているパスワード1211をディスク4より取り出し、内部データ暗号鍵120と内部データ暗号・復号化手段118により復号化して、ユーザが入力したパスワードと比較し、正規ユーザかどうかを確認する(ステップ7003、7004)。不正パスワードで一致しない場合ユーザにメッセージを出す等して警告し処理を終了する(ステップ7005)。一方、パスワードが一致した場合、は、ユーザ・インターフェイス1112は、ファイル復号化のためのウィンドウ表示処理を開始する。まず、暗号化されているファイルのリストをウィンドウ上に表示するため、ユーザ・インターフェイス1112は、ファイル復号化手段117に暗号化されたファイル名のリストを要求する。暗号化されたファイル名のリストに対する要求を受けると、ファイル復号化手段117は、ファイル名変更情報12131、12132と順次取り出し、それらを内部データ暗号鍵120と内部データ暗号・復号化手段118により復号化していく。そして、現在選択されている暗号化メタファに関連する暗号領域121上にある全てのファイル名変更情報を取得したところで、暗号化されているファイルの元の平文ファイル名のリストを作成し(ステップ7006)、ユーザ・インターフェイス1112に返す。復号化を行った暗号領域121上にある全てのファイル名変更情報は、後で、ファイル復号化する際に使うため、適当なバッファに保持しておく。ユーザ・インターフェイス1112は、暗号化された平文ファイル名のリストを受け取ると、ウィンドウ上にそのリストを表示する(ステップ7007)。次に、ウィンドウ上の暗号化された平文ファイル名のリストからユーザが復号化するファイルを選択すると(ステップ7008)、ユーザ・インターフェイス1112

(10)

特開平9-204330

17

は、選択されたファイル名のリスト作成し、それをファイル復号化要求と共に、ファイル復号化手段117に渡す。ファイル復号化手段117は、ファイル復号化要求を受け取ると、まず、ファイル暗号鍵1212を読みだし、内部データ暗号鍵120と内部データ暗号・復号化手段118によりファイル暗号鍵1212を復号化しておく。その後、ファイル復号化要求と、一緒に受け取った、ユーザが選択したファイル名のリスト上のファイル名を順次取り出し、全暗号化ファイルのリスト作成時に復号化してバッファに保持しておいたファイル名変更情報の平文ファイル名から一致するファイル名を検索し、暗号ファイル・データ領域151に格納された暗号ファイル名に変換する(ステップ7009)。そして、この暗号ファイルに対応したファイル位置情報を暗号データ領域121上のファイル位置情報から取得し元のファイルのディスク4上での位置を特定する(ステップ7010)。さらに、変換した暗号ファイル名の暗号ファイルのデータを暗号ファイル・データ151から読みだし、復号化しておいたファイル暗号鍵1212を用いて、データ暗号・復号化手段119により復号化し、ディスク4の元の位置に平文ファイルとして格納する(ステップ7011)。これらファイル復号化手段117のステップ7009～ステップ7011の処理をユーザが選択したファイル全てに対して繰り返す(ステップ7012)。以上がファイルの復号化処理である。

【0052】上記図7～9の各処理は、それぞれ個別に、または、一括して、計算機が読み取り可能なディスクや半導体メモリにプログラムの形で記述することができる。その様態も本発明に含まれる。

【0053】次に、パーソナル・コンピュータ上で、Graphical User Interface (以下、GUIと称す)によるユーザ・インターフェイスを実現する米国マイクロソフト社のオペレーティング・システム“MS-Windows” (MS-Windowsは米国マイクロソフト社の登録商標)に本発明を適用した一実施例におけるユーザ・インターフェイスについて、画面の具体的なイメージを示す図を用いて説明する。

【0054】また、本実施例では、日常生活においてセキュリティ機能を実現する道具としては最も一般的な金庫を模倣した“金庫フォルダ”をファイル暗号化メタファとして実現した。このような日常性のあるものをメタファに使うことにより、簡便操作と合わせてエンドユーザにも気軽に、高度なセキュリティ機能を操作できるようにした。

【0055】図10は、ファイル暗号化メタファの登録機能を実現する金庫フォルダ登録/削除ユーティリティのウィンドウのイメージを示したものである。ユーザが、新規登録ボタンをマウスで指して選択し、マウスのボタンを押下し、すぐ離す操作(以後、マウスで指して選択し、マウスのボタンを押下し、すぐ離す操作をクリックと称す)により、金庫フォルダの新規登録に起動を

18

かけると、図11に示す新規フォルダ登録ウィンドウを表示する。

【0056】本実施例では、図6の実施例で説明したように、複数の暗号化メタファの登録を実現する。そのために、図11の新規フォルダ登録ウィンドウでは、複数の金庫フォルダを登録した場合に、ユーザがそれぞれのフォルダの区別を付けるための、フォルダ名称の入力を行うようにした。また、図11の新規フォルダ登録ウィンドウでは、ユーザの認証、および、暗号鍵を生成するためのベースとなるパスワード入力を行う。入力ミスを防止するためにパスワードの再入力要求も出す。

【0057】図12は、前記の新規フォルダ登録操作により、金庫フォルダのメタファとして金庫の形をしたアイコンが、MS-Windowsのプログラム実行ユーティリティであるプログラム・マネージャに登録された状態を示す。新規フォルダ登録操作を繰り返し、複数の金庫フォルダを登録すると、金庫フォルダ一覧ウィンドウには、アイコン下部の名前の異なる複数の金庫フォルダ・アイコンが登録される。

【0058】図13は、図10と同じ金庫フォルダ登録/削除ユーティリティのウィンドウで、既に、登録してある金庫フォルダを削除する操作を示したものである。図の様に登録してある金庫フォルダの名前を登録フォルダ一覧を示す表示エリアで、マウスによりクリックして金庫フォルダを選択し、削除ボタンを選択すると、図14のフォルダ削除ウィンドウが表示される。そこで、金庫フォルダ登録時に入力したパスワードを入力すると金庫フォルダは、削除される。この削除機能は、図6のブロック図で示した実施例では便宜上説明しなかったが、削除した金庫フォルダに対応した暗号データ領域のファイル、および、暗号ファイル領域のディレクトリとその下の暗号ファイルを削除することにより実現できる。

【0059】ところで、図12の状態では、暗号化、および、復号化を行うプログラムをプログラム・マネージャに登録したもの、まだ、実行はされていない。しかし、一旦、プログラム・マネージャに金庫フォルダ・アイコンが登録されると、例えば、金庫フォルダ一覧ウィンドウ上の金庫フォルダ・アイコンをマウスで2回連続にクリック操作(以後、マウスで2回連続にクリック操作することをダブル・クリックと称す)することで、金庫フォルダの暗号化、および、復号化を行うプログラムを実行することができる。図15は、上記の操作で、金庫フォルダのプログラム実行した場合、金庫フォルダ・アイコンを示したものである。実行時の金庫フォルダのアイコンは、一般のプログラムの実行状態と同様に、MS-Windowsの背景となる壁紙領域に表示される。この状態で、金庫フォルダ・アイコンを操作することにより非常に簡便にファイル暗号化、復号化が可能となる。

【0060】図16は、実行状態の金庫フォルダ・アイコンより、複数のファイルの暗号化を行った画面を示し

19

たものである。まず、MS-Windowsのファイル管理ユーティリティであるファイル・マネージャのファイル名のリストを表示するウィンドウ上で、選択する複数のファイル名の上をマウスを押下しながら移動し、選択ができたところで離す（マウスのボタンを押下しながらマウス移動し、マウスを離す操作を以後ドラッグ・アンド・ドロップと称す）操作により、暗号化対象の複数のファイルを選択しておく。選択したファイル群で、再び、ドラッグ・アンド・ドロップ操作を開始し、金庫フォルダ上で、ドロップ（マウスのボタン離す操作）を行うだけで、選択した複数のファイルが暗号される。このように、金庫フォルダを使えば、実行してアイコン表示の状態にしておくだけで、ファイル・マネージャ等を介して、ドラッグ・アンド・ドロップという極めて簡便な操作でいつでもファイルを暗号化できる。また、図6のブロック図の実施例でも説明したように、金庫ファイルという暗号化メタファ登録時に、ユーザの認証に用いるパスワードから内部で自動的に暗号鍵を生成するため、ユーザが暗号鍵を意識しなくてすむことと、暗号化の際には、暗黙にその暗号鍵を用いて暗号化するため、ユーザ認証を必要としないことが操作の簡便化に非常に効果的である。これにより、例えば、金庫フォルダをMS-Windows実行時に自動的に実行される様にしておけば、ユーザは、プライベートな情報のメモや業務に関連した機密文書を作成した場合にいつでも気軽にこれら情報ファイルを、暗号鍵を用いた高度な暗号化機能により暗号化し、第三者にのせられる心配なく保存できるので非常に便利である。

【0061】もちろん、気軽に暗号化可能なために不用意に暗号化してしまう心配を持つユーザに対しての、例えば、金庫フォルダ実行後、最初の暗号化操作の場合のみパスワードによる認証を行う等の機能についても、図6のブロック図において、ファイル暗号化のユーザ・インターフェイス1111に暗号化処理の回数をカウントするカウンタを設け、最初に暗号化処理に起動がかかった場合にのみユーザ認証手段115によってユーザ認証を行うことで容易に実現可能であり、また、こうした、動作の選択を金庫フォルダの登録時の選択肢としてユーザに選択させることができる。

【0062】次に、本実施例では、図15の状態で、金庫フォルダをダブル・クリックすることによりファイルの復号化処理を起動するようにした。金庫フォルダをダブル・クリックすると図17のパスワード入力ウィンドウを表示するユーザが、金庫フォルダ登録時に指定したパスワードと一致していれば図18のファイル復号化ウィンドウがオープンできる。言うまでもなく、パスワードが間違っていれば、ファイル復号化ウィンドウをオープンできないので、パスワードを知らない第三者は、暗号化したファイルにアクセスすることはできない。

【0063】図18のようにファイル復号化ウィンドウでは、既に、暗号化して金庫フォルダに格納してあるフ

(11)

特開平9-204330

20

ァイルのリストを表示する。ファイルの復号化は、この暗号化したファイルのリスト上で、復号化したいファイル名をマウスでクリックして、図19に示すように、選択した後、取り出しボタンをクリックし、ディスク上の暗号化前に格納されていたディレクトリに元の平文に戻して格納する。また、同じように、マウスによりファイルを選択して、図20の様に削除ボタンをクリックすることで、ファイルの削除を行えるようにした。

【0064】この復号化ウィンドウのリストで参照しないと、暗号化したファイルは、図6のブロック図の実施例でも説明したように平文の時のファイル名をシリアル番号等によるファイル名に変更しているために、ファイル・マネージャ等のファイル管理ユーティリティで、金庫フォルダの暗号ファイル領域151等を覗いても何のファイルかもわからないのでより機密性を保持している。

【0065】

【発明の効果】本発明によれば、計算機の仕組みや操作に精通しないエンドユーザでも直感的で簡便な操作により、気軽にファイル等のデータの暗号化・復号化を活用することが可能であり、計算機上の個人情報や業務に関連した機密情報等のセキュリティの向上を容易に図ることが可能となる。

【図面の簡単な説明】

【図1】本発明の一実施例を示すブロック図である。

【図2】本発明を適用する基本的なシステム構成を示すブロック図である。

【図3】本発明の別の実施例を示すブロック図である。

【図4】本発明の別の実施例を示すブロック図である。

【図5】本発明の別の実施例を示すブロック図である。

【図6】本発明の別の実施例を示すブロック図である。

【図7】ファイル暗号化メタファ登録処理の手順を示すフローチャートである。

【図8】ファイル暗号化処理の手順を示すフローチャートである。

【図9】ファイル復号化処理の手順を示すフローチャートである。

【図10】本発明の一実施例である金庫フォルダ登録／削除ユーティリティ・ウィンドウを示す図である。

【図11】金庫フォルダの新規フォルダ登録ウィンドウを示す図である。

【図12】金庫フォルダが登録されたプログラム・マネージャのウィンドウを示す図である。

【図13】本発明の一実施例である金庫フォルダ登録／削除ユーティリティ・ウィンドウを示す図である。

【図14】金庫フォルダのフォルダ削除ウィンドウを示す図である。

【図15】金庫フォルダを実行した場合のアイコンを示す図である。

【図16】ファイル・マネージャを介して、金庫フォル

(12)

特開平9-204330

21

22

ダでファイルの暗号化を行う操作画面を示す図である。

【図17】金庫フォルダでウィンドウをオープンするためのパスワード入力ウィンドウを示す図である。

【図18】金庫フォルダの復号化ウィンドウを示す図である。

【図19】金庫フォルダの復号化ウィンドウでのファイルの復号化操作を示す図である。

【図20】金庫フォルダの復号化ウィンドウでのファイルの削除操作を示す図である。

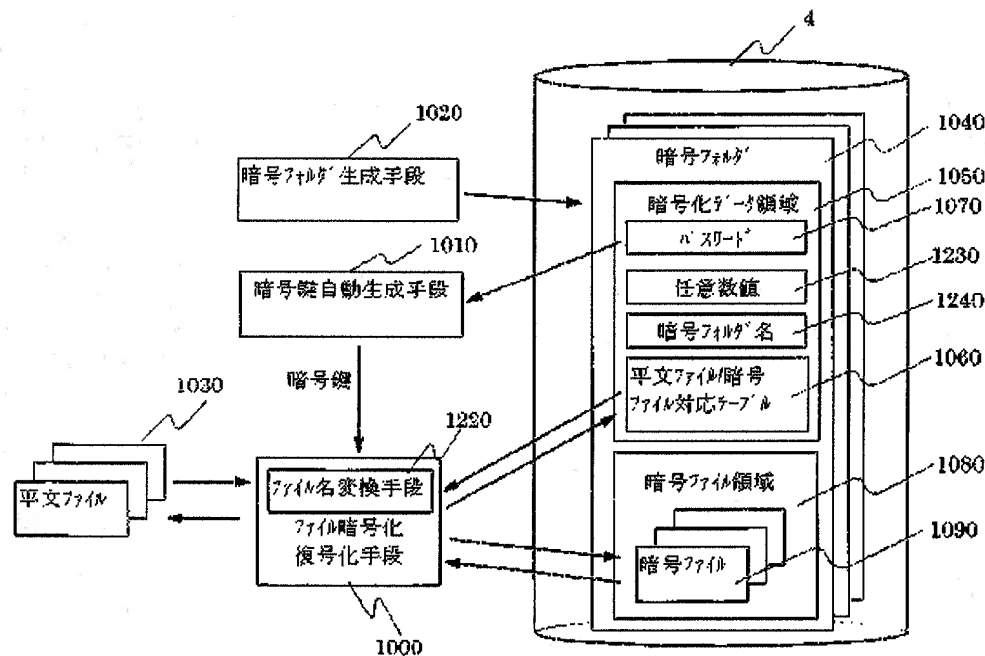
【符号の説明】

1…CPU、2…ROM、3…RAM、4…ディスク、5…ディスプレイ、6…キーボード、7…マウス、8…システム・バス、11…ファイル暗号化制御、111…ユーザ・インターフェイス、112…ファイル暗号化領域生成手段、113…パスワード登録手段、114…暗号鍵生成登録手段、115…ユーザ認証手段、116…ファイル暗号化手段、117…ファイル復号化手段、118…内部データ暗号・復号化手段、119…データ暗号・復号化手段、12…ファイル暗号化制御データ、121、122、123…暗号化データ領

域、13…ファイル管理手段、141、142…平文ファイル、151、152、153…暗号ファイル領域、1000…ファイル暗号化復号化手段、1010…暗号鍵自動生成手段、1020…暗号フォルダ生成手段、1030…平文ファイル、1040…暗号フォルダ、1050…暗号化データ領域、1060…平文ファイル/暗号ファイル対応テーブル、1070…パスワード、1080…暗号ファイル領域、1090…暗号ファイル、1100…暗号フォルダ・ファイル生成手段、1110…暗号フォルダ生成手段、1120…暗号フォルダ・ファイル、1130…暗号ファイル領域データ、1140…自己復号化プログラム生成手段、1150…復号化プログラム、1160…自己復号化プログラム、1170…復号化手段、1180…認証手段、1190…カウンタ、1200…暗号フォルダ無効化手段、1210…暗号フォルダバックアップ手段、1230…任意数値、1240…暗号フォルダ名、1220…ファイル名交換手段、1300…F D、1400…ネットワーク

【図1】

図1

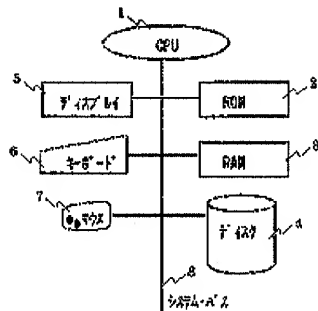


(13)

特開平9-204330

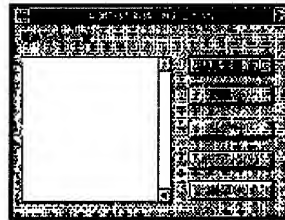
【図2】

図2



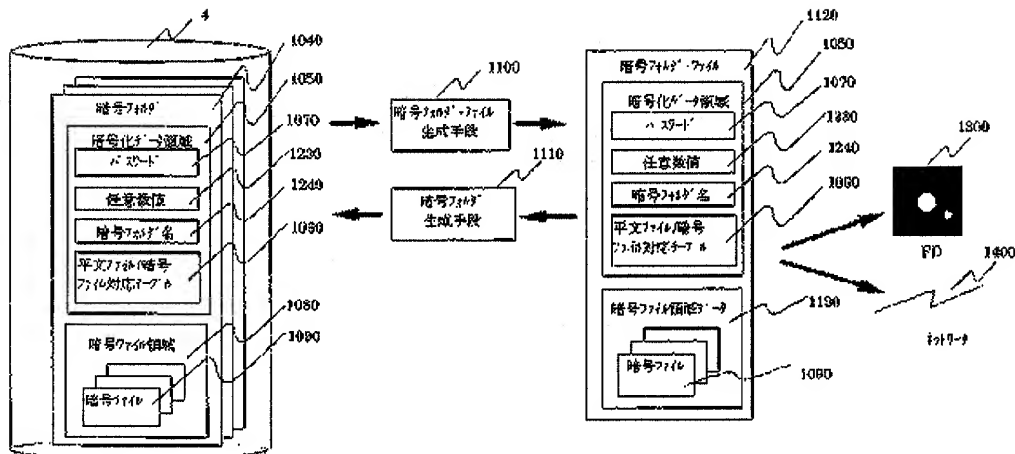
【図10】

図10



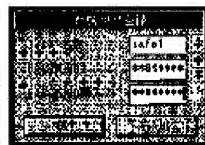
【図3】

図3



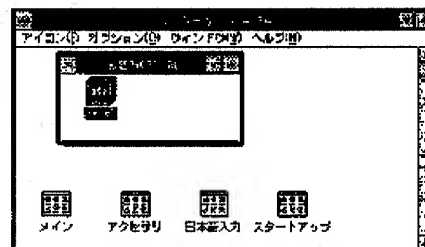
【図11】

図11



【図12】

図12



【図15】

図15



(14)

特開平9-204330

【図4】

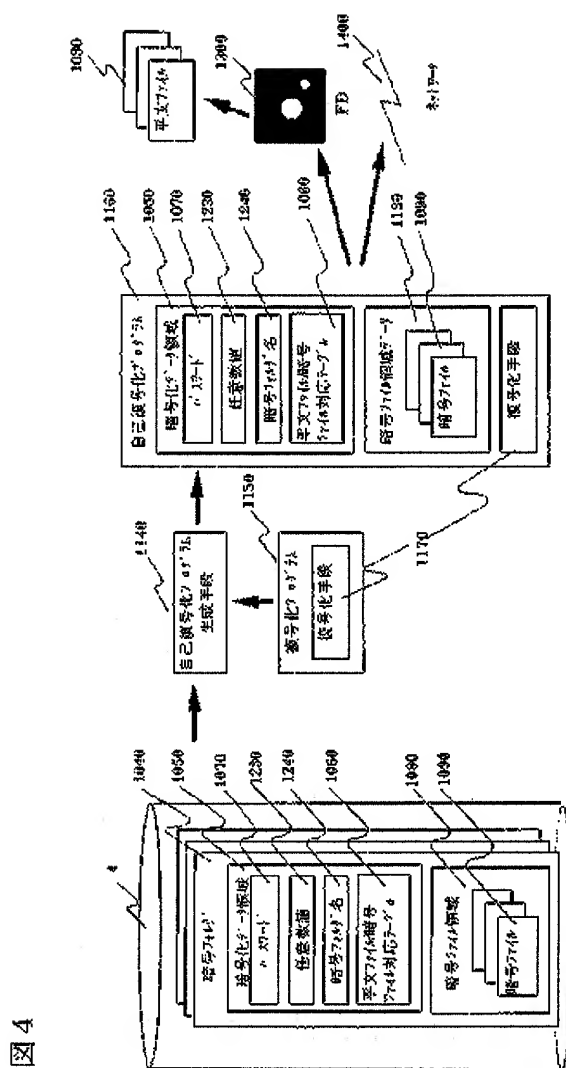
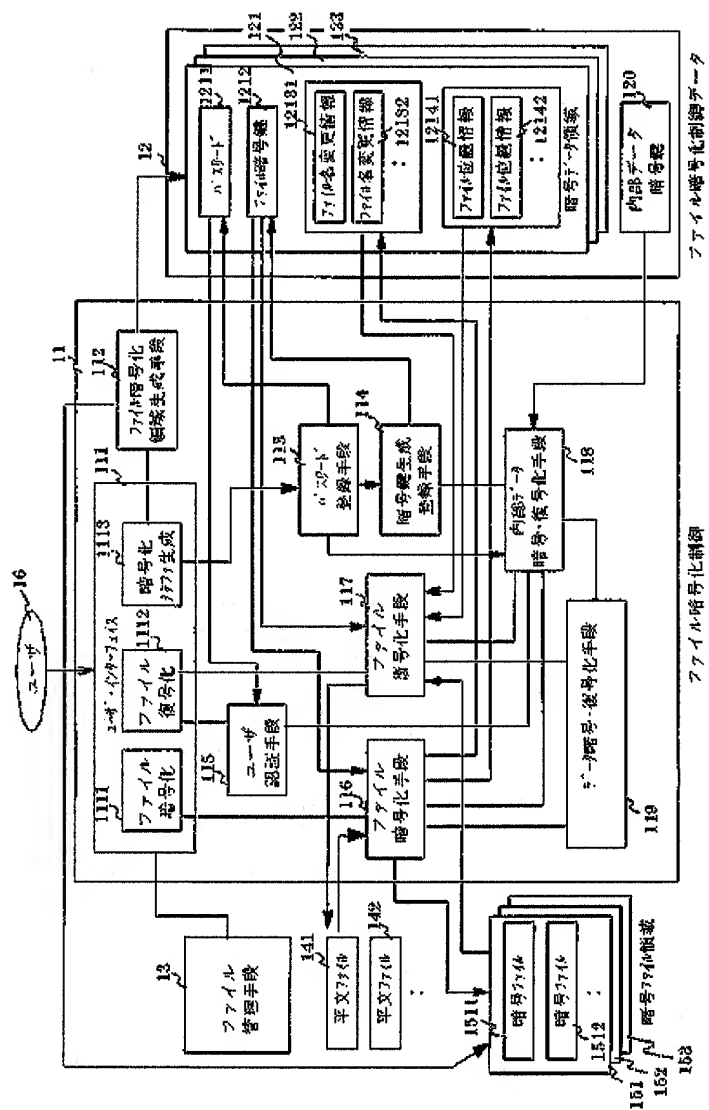


図4

特開平9-204330



(17)

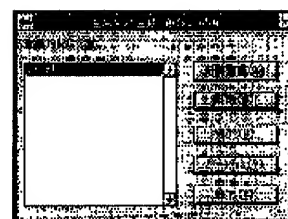
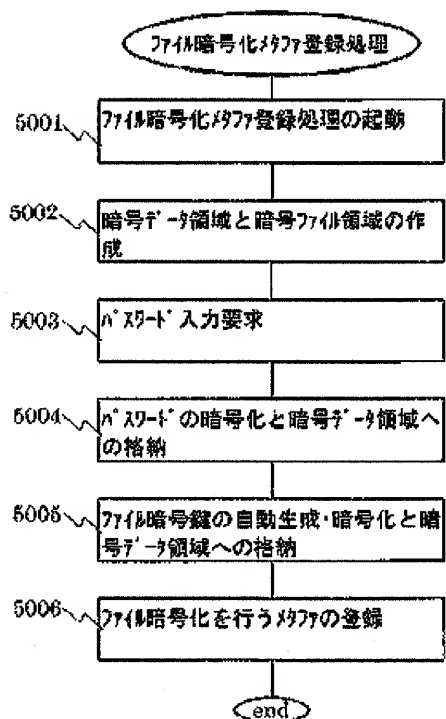
特開平9-204330

【図7】

【図13】

図7

図13



【図17】

図17

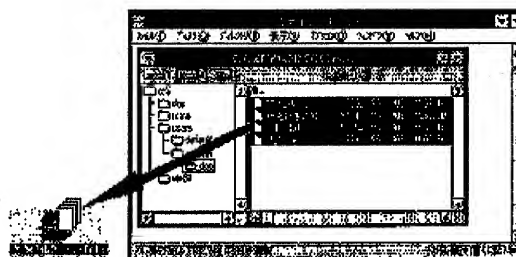


【図14】

【図16】

図14

図16

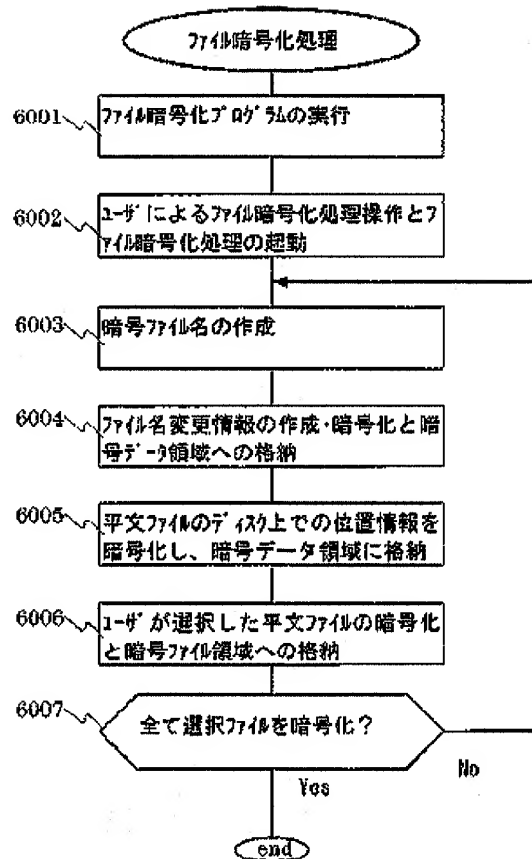


(18)

特開平9-204330

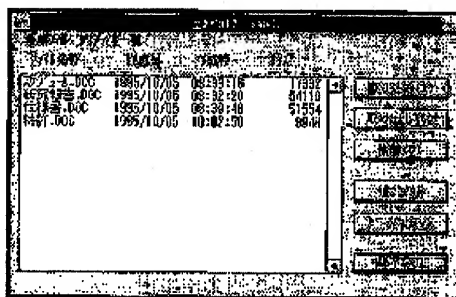
【図8】

図8



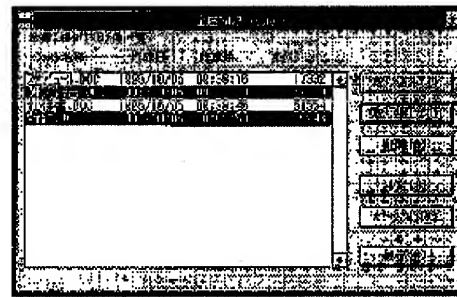
【図18】

図18



【図19】

図19

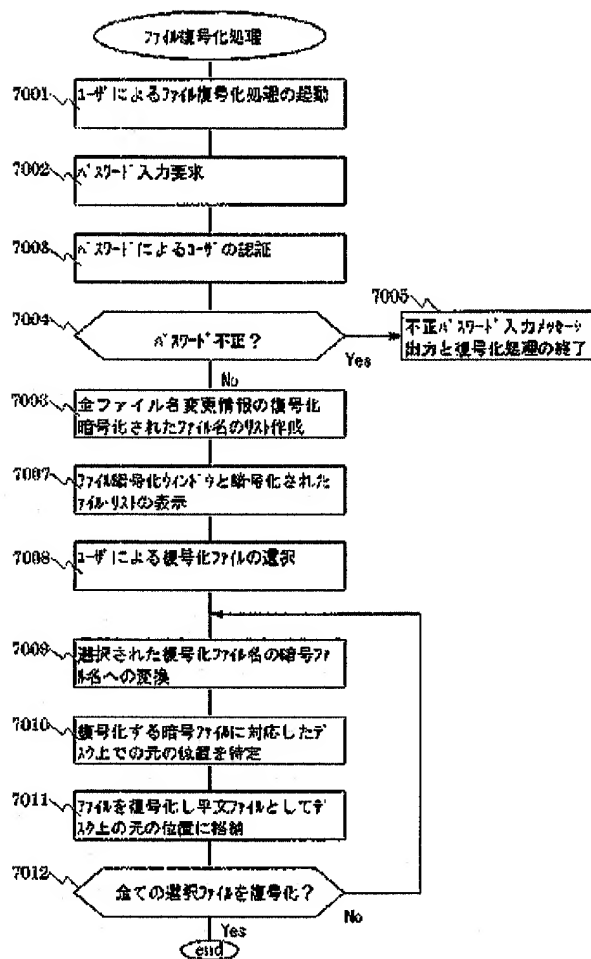


(19)

特開平9-204330

【図9】

図9

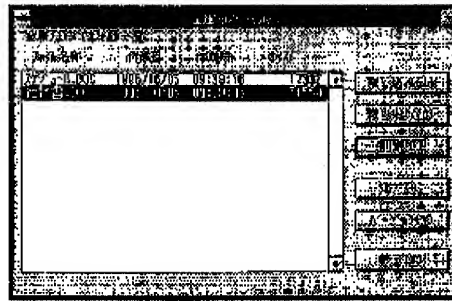


(20)

特開平9-204330

【図20】

図20



フロントページの続き

(51)Int.Cl. ⁹	識別記号	序内整理番号	F I	技術表示箇所
G 0 9 C 1/00	6 3 0	7259-5J	G 0 9 C 1/00	6 3 0 Z
	6 6 0	7259-5J		6 6 0 D
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 A
9/32				6 0 1 Z
				6 7 3 A

(72)発明者 古川 紳
 神奈川県川崎市麻生区王禅寺1099番地株式
 会社日立製作所システム開発研究所内

(72)発明者 住友 正人
 神奈川県海老名市下今泉810番地株式会社
 日立製作所オフィスシステム事業部内

(72)発明者 小林 祐一
 神奈川県海老名市下今泉810番地株式会社
 日立製作所オフィスシステム事業部内